REMARKS

Claims 1-5, 7-9, 11-13, 15 and 16 are pending in this application, and, in the Office Action, the Examiner rejected all of these claims under 35 U.S.C. 102 as being fully anticipated by U.S. Patent 7,013,296 (Yemini, et al.) Both of the previous rejections of the claims under 35 U.S.C. 112 and under 35 U.S.C. 103 were withdrawn.

The rejection of the claims under 35 U.S.C. 102 is respectfully traversed. Also, editorial changes are being made to Claims 1, 3, 7 and 11, and new Claim 17, which is dependent from Claim 1.

For the reasons explained below, Claims 1-5, 7-9, 11-13, 15 and 16 patentably distinguish over the prior art and are allowable. The Examiner is thus asked to reconsider and to withdraw the rejections of Claims 1-5, 7-9, 11-13, 15 and 16 under 35 U.S.C. 102 and to allow these claims.

As explained in detail in the present application, the instant invention provides a procedure to create and to use electronic cash. With a preferred embodiment of the invention, a customer sends to a bank a request for digital cash and a public key of an encryption scheme of the customer. The bank signs the cash using a secret key of the bank's own digital signature scheme, and encrypts the signature by using the public key provided by the customer. The bank also encrypts, using the public key given to the bank by the customer, an unsigned copy of the cash. A copy of the encrypted signed cash and a copy of the encrypted unsigned cash are both sent to the customer by the bank.

The customer then decrypts both of these copies – that is, both the signed and unsigned copies of the cash - by using the private key of the customer's encryption scheme. The customer then uses this decrypted, signed and unsigned pair of copies for payment to a third party. The

third party, using these decrypted signed and unsigned copies of the cash, can then ask the bank to confirm the validity of the digital cash. If that validity is confirmed, this third party is able to redeem the digital cash for payment.

An important feature of the present invention is that the bank encrypts both the signed and unsigned copies of the digital cash using the public key of the customer's encryption scheme – that is, the customer has the private key of that encryption scheme. Then, both encrypted copies – that is, the encrypted copy of the signed coin and the encrypted copy of the unsigned coin - are sent back to the customer. Because of this feature, the customer, and only the customer, is able to decrypt both the signed and unsigned copies of the digital cash by using the private key of the customer's encryption scheme. In this way, only the customer is able to control the use of these copies.

The prior art of record does not disclose or suggest this feature of the present invention.

In particular, Yemimi, et al. describes an electronic payment system, and is particularly directed to enhancing the security of that system. As part of this system, a banking infrastructure is provided for generating and managing access rights in the system. In this banking infrastructure, shown in Figure 7 and discussed in detail in columns 27-31, mint bank 42 generates currency, and cryptographic techniques are used to help assure that the currency is not forgeable. More specifically, another bank, referred to as an exchange bank, presents the mint bank with a group of security values. The mint bank creates new security values that are returned to the exchange bank. The newly generated currency is signed by the mint bank.

As noted in column 30 of Yemini, et al, the mint bank has a public key 74 for encryption purposes. There is no disclosure in Yemini, et al, though, that this public key is used to encrypt the currency sent back to the exchange bank. Nor is there any teaching that public key is part of

a public key/private key encryption scheme of that exchange bank or that this public key is given to the mint bank by the exchange bank.

In the Office Action, the Examiner cited Yemini, et al. column 30, line 62 to column 31, line 55, as disclosing, among other matters, sending back to the user both the encrypted copy of the signed coin and the encrypted copy of the unsigned coin. A careful review shows, however, that this portion of Yemini, et al. does not disclose sending these two encrypted coins back to a user. In particular, this section of Yemimi, et al. discusses Figure 15, which shows the information maintained in the exchange bank log. This information includes, among other items, spending behavior statistics, liability transfer information, bill deposit information, buying behavior statistics, and recent exchange activity. There is no teaching, though, of sending encrypted copies of two coins, - one signed by the bank and one unsigned by the bank – to the user.

Independent Claims 1, 3, 7 and 11 clearly describe important features of this invention that are not shown in or suggested by Yemini, et al. In particular, Claims 1 and 7 describe the features that encrypted copies of the signed and unsigned coins are encrypted using the public key of an encryption scheme, that both of these copies are sent back to the user or customer, and that the user or the customer uses the private key of this encryption scheme to decrypt both the signed and unsigned copies of the coin. Claims 1 and 7 also describe the feature that the user or customer uses that pair of coins - that is, the signed and unsigned copies of the coin - as digital cash. Claim 7 add the further limitation that this pair of coins is used as a payment to a recipient.

Claims 3 and 11, as presented herein, describe the features that the secure cryptography generator encrypts both the signed unit and the unsigned unit using the public key of the given encryption scheme communicated to the cryptography generator from the customer. As further

described in these claims, this pair of encrypted coins are transmitted back to the customer, decrypted by the customer, and used as a unit as payment to a recipient, and this recipient then presents this pair of coins to the bank for credit.

The other references of record have been reviewed, and these other references, whether considered individually or in combination, also do not disclose or suggest encrypting the pair of coins, or this use of the pair of subsequently decrypted signed and unsigned coins, as described in Claims 1, 3, 7 and 11.

For instance, U.S. Patent 6,311,171 (Dent), which was previously cited by the Examiner, discloses a procedure for providing secure electronic communications. In this procedure, coins are encrypted by a bank using the owner's secret key. The encrypted coins are sent back to the owner, who can decrypt them using a public key and then can use the coins as payment.

U.S. Patent 5,832,089 (Kravitz, et al.), also previously cited by the Examiner, describes a procedure for handling electronic cash. With this procedure, a customer is provided with encrypted copies of a signed and unsigned coin. These are decrypted by the customer using a secret key, and the decrypted signed unit can then be used as a payment.

In light of the differences between Claims 1, 3, 7 and 11 and the prior art, and because of the advantages associated with those differences, these claims patentably distinguish over the prior art and are allowable. Claim 2 is dependent from Claim 1 and is allowable therewith; and Claims 4, 5, 15 and 16 are dependent from Claim 3 and are allowable therewith. Also, Claims 8 and 9 are dependent from Claim 7 and are allowable therewith; and Claims 12 and 13 are dependent from, and are allowable with, Claim 11.

For the reasons discussed above, the Examiner is asked to reconsider and to withdraw the rejections of Claims 1-5, 7-9, 11-13, 15 and 16 under 35 U.S.C. 102, and to allow these claims. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is requested to telephone the undersigned.

Respectfully submitted,

John S. Sensny

John S. Sensny
Registration No. 28,757
Attorney for Applicants

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza - Suite 300
Garden City, New York 11530
(516) 742-4343

JSS:jy